

REMARKS

Claims 1-38 are pending in this application. By this Amendment, claims 1, 5, 7 and 20 are amended to better distinguish over the prior art. Reconsideration is respectfully requested.

It is gratefully appreciated that the Office Action indicates that claims 21-38 are allowed. The courtesy extended to Applicant's representative during the April 25 telephonic interview with Examiner Kim is gratefully appreciated. During the telephonic interview, Examiner Kim indicated that claims 21-38 are allowed because the prior art of record fails to disclose at least holding a certificate C to prove a public key y paired with the one-way function value $X(M)$. The Examiner also indicated that the prior art fails to show at least a means for creating an access ticket t from a private key x and the one-way function value $X(M)$. The points discussed during the telephonic interview are reemphasized in this Amendment.

The Office Action rejects claims 1, 2, 5-10, 19 and 20 under 35 U.S.C. §103(a) over Zhang (U.S. Patent No. 6,154,541); claim 18 under 35 U.S.C. §103(a) over Zhang and Stallings ("Cryptography and Network Security"); and claims 3, 4 and 11-17 under 35 U.S.C. §103(a) over Zhang and Schneier ("Applied Cryptography"). The rejections are respectfully traversed.

In particular, the applied references do not disclose or suggest a method for generating a one-way function dependent on a one-way function H and a unique value d for a user, including at least holding a certificate C to prove a public key y paired with the one-way function value $X(M)$, as recited in independent claim 1, and similarly recited in independent claim 5. Furthermore, the applied references do not disclose or suggest a proving device, including at least a means for inputting a message M , the message M including at least identifiers of private key processing algorithms, wherein the identifiers in the message M

enable the private key processing algorithms to be modified, as recited in independent claim 7. Finally, the applied references do not disclose or suggest a device for issuing a proving instrument T, including at least a means for issuing the proving instrument T that includes a hash function X dependent on the unique value d, as recited in independent claim 20.

Specifically, as discussed during the April 25 telephonic conference, the applied references failed to disclose holding a certificate C to prove a public key y paired with the one-way function value $X(M)$. Thus, claims 1-6 should be in a condition for allowance.

Zhang discloses a cryptographic system that encrypts a cipher text C by a key vector K_c . Stallings discloses a certificate authentication method. Schneier discloses encryption and decryption protocols.

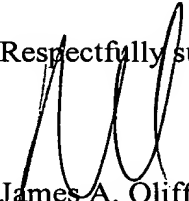
However, the applied references fail to disclose or suggest at least holding a certificate C to prove a public key y paired with the one-way function value $X(M)$. Furthermore, the applied references do not disclose or suggest at least a message M including at least identifiers of private key processing algorithms, the identifiers in the message M enable the private key processing algorithms to be modified. Finally, the applied references fail to disclose or suggest at least a means for issuing the proving instrument T that includes a hash function X dependent on the unique value d. On the contrary, nowhere in the applied references are these features disclosed or suggested.

Accordingly, any combination of the applied references would not have resulted in a device that provides lower center management costs and minimizes the disclosure of private information. Because it would not have been obvious to modify the applied references to arrive at the claimed invention, it is respectfully requested that the rejections under 35 U.S.C. §103(a) be withdrawn.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of the claims are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,


James A. Oliff
Registration No. 27,075

Richard S. Elias
Registration No. 48,806

JAO:RSE/eks

Date: April 29, 2005

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

<p>DEPOSIT ACCOUNT USE AUTHORIZATION Please grant any extension necessary for entry; Charge any fee due to our Deposit Account No. 15-0461</p>
